Αναφορά σχετικά με τις απαιτήσεις ασφάλειας δεδομένων, ασφάλειας συστήματος και GDPR

Εισαγωγή

Ο σκοπός αυτής της έκθεσης είναι να παρουσιάσει μια επισκόπηση των απαιτήσεων Ασφάλειας Δεδομένων, Ασφάλειας Συστήματος και GDPR που σχετίζονται με το έργο του ΔΕΔΔΗΕ. Αυτή η έκθεση στοχεύει να παρέχει μια λεπτομερή ανάλυση σχετικά με τις βασικές εκτιμήσεις και τις ενέργειες που απαιτούνται για τη διατήρηση της συμμόρφωσης και τη διασφάλιση της ακεραιότητας του έργου. Η ενσωμάτωση με τις τεχνολογίες Azure θα τονιστεί για τη βελτίωση αυτών των απαιτήσεων.

Απαιτήσεις ασφάλειας δεδομένων

Η ασφάλεια των δεδομένων είναι πρωταρχικής σημασίας για την προστασία ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, παραβιάσεις και άλλες απειλές. Ακολουθούν οι κρίσιμες απαιτήσεις για την ασφάλεια των δεδομένων και πώς μπορούν να ενσωματωθούν οι τεχνολογίες Azure:

1. Κρυπτογράφηση δεδομένων

Κρυπτογράφηση σε κατάσταση ηρεμίας και κατά τη μεταφορά: Εφαρμογή μεθόδων κρυπτογράφησης όπως το AES-256 για την προστασία των δεδομένων που είναι αποθηκευμένα σε μονάδες δίσκου (σε κατάσταση ηρεμίας) και κατά τη μετάδοση μέσω δικτύων (σε μεταφορά).

- **Ενσωμάτωση Azure** : Χρησιμοποιήστε την κρυπτογράφηση υπηρεσίας αποθήκευσης Azure (SSE) για δεδομένα σε κατάσταση ηρεμίας και την κρυπτογράφηση εικονικού δικτύου Azure για δεδομένα υπό μεταφορά.
- Βιβλιογραφικές αναφορές:
  - Κρυπτογράφηση υπηρεσίας αποθήκευσης Azure
  - Κρυπτογράφηση εικονικού δικτύου Azure

2. Έλεγχος πρόσβασης

- **Έλεγχος πρόσβασης βάσει ρόλων (RBAC)** : Καθορισμός και επιβολή ρόλων και αδειών χρήστη για περιορισμό της πρόσβασης σε δεδομένα με βάση την αρχή του ελάχιστου προνομίου.
  - **Ενσωμάτωση Azure** : Εφαρμόστε το Azure RBAC για να διαχειριστείτε ποιος έχει πρόσβαση στους πόρους του Azure.
  - Βιβλιογραφικές αναφορές:
    - Έλεγχος πρόσβασης βάσει ρόλων Azure

- **Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA)** : Εφαρμογή MFA για την προσθήκη ενός επιπλέον επιπέδου ασφάλειας για την πρόσβαση σε ευαίσθητα δεδομένα, διασφαλίζοντας ότι οι χρήστες επαληθεύονται με πολλαπλές μεθόδους.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων Azure.
    - Βιβλιογραφικές αναφορές:
        - Azure Multi- Factor Authentication

3. Προστασία Δεδομένων

- **Τακτικά αντίγραφα ασφαλείας** : Διεξαγωγή συχνών αντιγράφων ασφαλείας δεδομένων και αποθήκευση τους με ασφάλεια για την αποφυγή απώλειας δεδομένων σε περίπτωση αστοχιών του συστήματος ή συμβάντων στον κυβερνοχώρο.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Backup για αξιόπιστα και ασφαλή αντίγραφα ασφαλείας.
    - Βιβλιογραφικές αναφορές:
        - Azure Backup
- **Απόκρυψη και ανωνυμοποίηση δεδομένων** : Χρήση τεχνικών για την ανωνυμοποίηση και απόκρυψη ευαίσθητων δεδομένων, μειώνοντας τον κίνδυνο έκθεσης κατά την επεξεργασία και ανάλυση δεδομένων.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε τη δυναμική κάλυψη δεδομένων βάσης δεδομένων Azure SQL και την ανάλυση Azure Data Lake για ανωνυμοποίηση.
    - Βιβλιογραφικές αναφορές:
        - Δυναμική κάλυψη δεδομένων βάσης δεδομένων Azure SQL
        - Azure Data Lake Analytics

4. Ακεραιότητα δεδομένων

- **Έλεγχοι ακεραιότητας** : Χρησιμοποιώντας αθροίσματα ελέγχου και κατακερματισμούς για την επαλήθευση της ακεραιότητας των δεδομένων, διασφαλίζοντας ότι παραμένουν αμετάβλητα και αμετάβλητα.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Blob Storage που υποστηρίζει κατακερματισμό MD5 για ακεραιότητα δεδομένων.
    - Βιβλιογραφικές αναφορές:

Commented [FS1]: Λόγο οτι τα data προερχονται απο άλλα συστήματα με δυνατότητα επαναφοράς σε περίπτωση απώλειας δεν υπάρχουν ιδιαίτερες απαιτήσεις backup στο έργο σε επίπεδο δεδομένων. Μας καλύπτει το ZRS του Azure storage account όπου τα data γινονται replicate και σε άλλα zones και ίσως και το LRS (Local redudant storage- 3x replication) να είναι αρκετο. Θα αποφασιστεί στην ανάλυση

Commented [KA2R1]: Συμφωνώ με το σχόλιο. Το ZRS του Azure καλύπτει τις απαιτήσεις επαναφοράς δεδομένων και ίσως το LRS να είναι αρκετό, όπως αναφέρεται στις τεχνικές προδιαγραφές των αρχείων "Architecture_utf8" και "AnyConv.com__IBM DATASTAGE - 4 GOLDEN RECORD"

Commented [FS3]: Πρέπει να αναλυθεί περισσότερο καθώς σε επίπεδο databricks/analytics δεν θα απαιτείτε anonymization (είναι αρκετά περίπλοκο) αλλά στα τελικα αποτελέσματα που θα μπορούν να βλέπουν οι χρήστες

Commented [KA4R3]: Συμφωνώ με το σχόλιο. Στο αρχείο "AnyConv.com__IBM DATASTAGE - 3 MATCHING PROCESS" αναφέρεται ότι η ανωνυμοποίηση πρέπει να γίνει στα τελικά αποτελέσματα που βλέπουν οι χρήστες.

Commented [FS5]: Εδω θα χρειαστεί custom hashing γιατί μιλάμε για integrity μεταξύ των layers επεξεργασίας, τα αρχεία δεν παραμένουν ίδια endtoend.

Commented [KA6R5]: Συμφωνώ με το σχόλιο. Στο αρχείο "Blocking and Matching criteria" αναφέρεται η ανάγκη για custom hashing για τη διατήρηση της ακεραιότητας των δεδομένων.

        - Κατακερματισμός Azure Blob Storage MD5

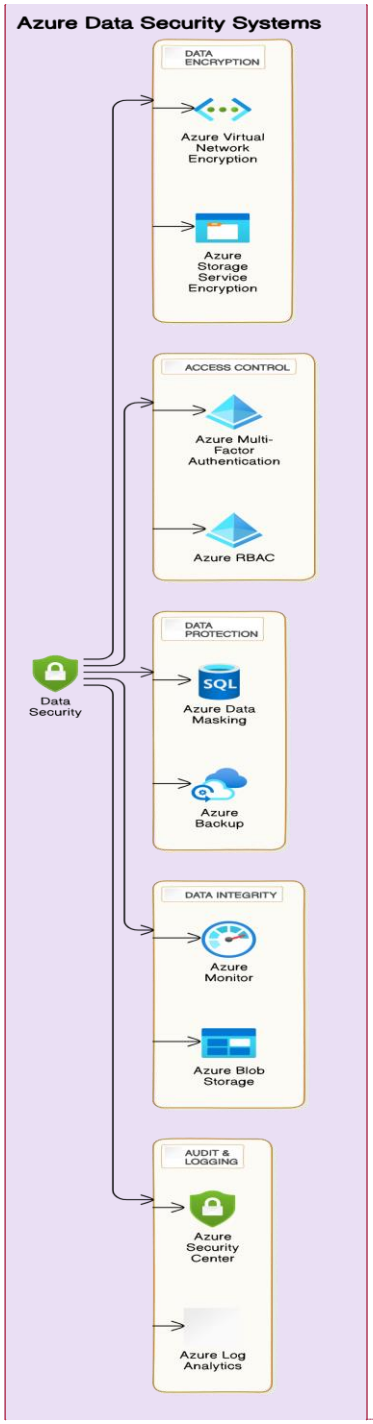
- **Πρόληψη μη εξουσιοδοτημένων τροποποιήσεων** : Εφαρμογή μηχανισμών για τον εντοπισμό και την πρόληψη μη εξουσιοδοτημένων τροποποιήσεων δεδομένων.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε την οθόνη Azure για να εντοπίσετε μη εξουσιοδοτημένες τροποποιήσεις.
    - Βιβλιογραφικές αναφορές:
        - Azure Monitor

5. Έλεγχος και Καταγραφή

- **Ολοκληρωμένη καταγραφή** : Διατήρηση λεπτομερών αρχείων καταγραφής πρόσβασης δεδομένων, τροποποιήσεων και μεταφορών για τη διευκόλυνση του ελέγχου και της εγκληματολογικής ανάλυσης.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Log Analytics για λεπτομερή καταγραφή.
    - Βιβλιογραφικές αναφορές:
        - Azure Log Analytics
- **Τακτικοί έλεγχοι** : Διενέργεια τακτικών ελέγχων για τη διασφάλιση της τήρησης των πολιτικών ασφάλειας δεδομένων και τον εντοπισμό πιθανών τρωτών σημείων.
    - **Azure Integration** : Χρησιμοποιήστε το Azure Security Center για συνεχή αξιολόγηση ασφάλειας.
    - Βιβλιογραφικές αναφορές:
        - Κέντρο Ασφαλείας Azure
- Ασφάλεια δεδομένων Azure

Commented [FS7]: Στο databricks δεν υποστηρίζεται κάτι τέτοιο, μπορούμε να το κάνουμε με hashing, όχι με azure functionality

Commented [KA8R7]: Συμφωνώ με το σχόλιο. Στο αρχείο "Technical_Prodiagrafes" αναφέρεται ότι το hashing είναι η προτιμώμενη μέθοδος για την υποστήριξη της λειτουργικότητας αυτής.



Commented [FS9]: Πρέπει να γίνει enrich προσθέτοντας τα επίπεδα databricks και πως χειριζόμαστε το security σε κάθε επίπεδο

Commented [KA10R9]: Συμφωνώ με το σχόλιο. Στο αρχείο "Architecture" αναφέρεται η ανάγκη για εμπλουτισμό των επιπέδων databricks και της διαχείρισης ασφάλειας σε κάθε επίπεδο

Απαιτήσεις ασφάλειας συστήματος

Η ασφάλεια του συστήματος περιλαμβάνει μέτρα για την προστασία της υποδομής του δικτύου, του υλικού και του λογισμικού από απειλές και τρωτά σημεία. Οι βασικές απαιτήσεις περιλαμβάνουν:

1. Ασφάλεια Δικτύου

- **Τείχη προστασίας και IDS/IPS** : Ανάπτυξη τειχών προστασίας και συστημάτων ανίχνευσης/αποτροπής εισβολής για την παρακολούθηση και τον έλεγχο της εισερχόμενης και εξερχόμενης κίνησης δικτύου με βάση προκαθορισμένους κανόνες ασφαλείας.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε το τείχος προστασίας Azure και την προστασία Azure DDoS.
    - Βιβλιογραφικές αναφορές:
        - Τείχος προστασίας Azure
        - Προστασία Azure DDoS
- **Secure Network Architecture** : Σχεδιασμός μιας ασφαλούς αρχιτεκτονικής δικτύου με τμηματοποίηση για την απομόνωση κρίσιμων συστημάτων και δεδομένων από πιθανές απειλές.
    - **Ενοποίηση Azure** : Χρησιμοποιήστε το εικονικό δίκτυο Azure για να δημιουργήσετε μεμονωμένα τμήματα δικτύου.
    - Βιβλιογραφικές αναφορές:
        - Εικονικό δίκτυο Azure

2. Ασφάλεια τελικού σημείου

- **Antivirus και Anti-Malware** : Εγκατάσταση και τακτική ενημέρωση λογισμικού προστασίας από ιούς και κακόβουλου λογισμικού για την προστασία των τελικών σημείων από κακόβουλες επιθέσεις.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Microsoft Defender για Endpoint.
    - Βιβλιογραφικές αναφορές:
        - Microsoft Defender για Endpoint
- **Επιδιορθώσεις συστήματος και ενημερώσεις** : Διασφάλιση ότι όλα τα συστήματα και το λογισμικό επιδιορθώνονται και ενημερώνονται τακτικά για τον μετριασμό των τρωτών σημείων.

Commented [FS11]: Πρέπει να γίνει πιο συγκλεκριμένο, πολλά απο αυτά πρέπει να καλύπτονται απο το infra του οργασνισμού και να δηλώσουμε τι θα είναι δικό μας responsibility στην υλοποίηση του έργου.

Commented [KA12R11]: Συμφωνώ με το σχόλιο. Στο αρχείο "AnyConv.com__IBM DATASTAGE - 4 GOLDEN RECORD" αναφέρεται η ανάγκη για σαφή οριοθέτηση των ευθυνών μεταξύ του οργανισμού και του έργου.

- **Ενσωμάτωση Azure** : Χρησιμοποιήστε τη Διαχείριση Ενημερώσεων Αυτοματισμού Azure.
- Βιβλιογραφικές αναφορές:
  - Διαχείριση ενημέρωσης αυτοματισμού Azure

3. Φυσική Ασφάλεια

- **Έλεγχοι πρόσβασης** : Εφαρμογή φυσικών ελέγχων πρόσβασης σε κέντρα δεδομένων και διακομιστές, συμπεριλαμβανομένων βιομετρικών σαρωτών και συστημάτων καρτών-κλειδιών.
  - **Ενσωμάτωση Azure** : Τα κέντρα δεδομένων Azure ακολουθούν αυστηρά πρωτόκολλα φυσικής ασφάλειας.
  - Βιβλιογραφικές αναφορές:
    - Φυσική ασφάλεια Azure Datacenter
- **Επιτήρηση και παρακολούθηση** : Χρήση καμερών παρακολούθησης και συστημάτων παρακολούθησης για την ασφάλεια φυσικών τοποθεσιών και τον εντοπισμό μη εξουσιοδοτημένης πρόσβασης.
  - **Ενσωμάτωση Azure** : Τα κέντρα δεδομένων Azure είναι εξοπλισμένα με συστήματα επιτήρησης.
  - Βιβλιογραφικές αναφορές:
    - Azure Datacenter Surveillance

4. Ασφάλεια Εφαρμογών

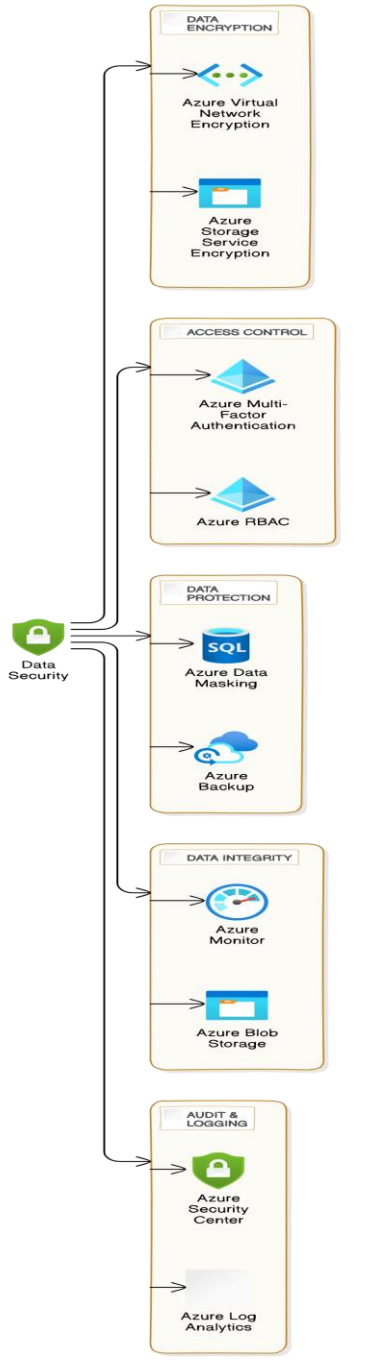
- **Πρακτικές Ασφαλούς Ανάπτυξης** : Υιοθέτηση προτύπων ασφαλούς κωδικοποίησης, διεξαγωγή ελέγχων κώδικα και εφαρμογή δοκιμών ασφαλείας σε όλο τον κύκλο ζωής ανάπτυξης λογισμικού.
  - **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure DevOps για ασφαλείς αγωγούς CI/CD.
  - Βιβλιογραφικές αναφορές:
    - Azure DevOps
- **Εκτιμήσεις ευπάθειας** : Διεξαγωγή τακτικών αξιολογήσεων ευπάθειας και δοκιμών διείσδυσης για τον εντοπισμό και την αποκατάσταση αδυναμιών ασφάλειας.
  - **Azure Integration** : Χρησιμοποιήστε το Azure Security Center για αξιολογήσεις ευπάθειας.
  - Βιβλιογραφικές αναφορές:

        - Κέντρο Ασφαλείας Azure

5. Αντιμετώπιση περιστατικού

- **Σχέδιο Αντιμετώπισης Συμβάντων** : Ανάπτυξη και διατήρηση ενός ολοκληρωμένου σχεδίου αντιμετώπισης συμβάντων για την αποτελεσματική αντιμετώπιση και άμβλυνση περιστατικών ασφαλείας.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Sentinel για ανίχνευση και απόκριση περιστατικού.
    - Βιβλιογραφικές αναφορές:
        - Azure Sentinel
- **Εκπαίδευση και ασκήσεις** : Διεξαγωγή τακτικών εκπαιδευτικών συνεδριών και ασκήσεων για την ομάδα αντιμετώπισης περιστατικών για να διασφαλιστεί η ετοιμότητα για πιθανές παραβιάσεις της ασφάλειας.
    - **Azure Integration** : Αξιοποιήστε τους πόρους εκπαίδευσης της Microsoft για την απόκριση σε περιστατικά.
    - Βιβλιογραφικές αναφορές:
        - Microsoft Training
- **Ασφάλεια συστήματος Azure**

Data Security Systems on Azure



-

Απαιτήσεις GDPR

Η συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR) είναι απαραίτητη για την προστασία των προσωπικών δεδομένων και τη διασφάλιση των δικαιωμάτων των υποκειμένων των δεδομένων. Οι βασικές απαιτήσεις GDPR περιλαμβάνουν:

1. Δικαιώματα υποκειμένου δεδομένων

- **Αιτήματα πρόσβασης** : Εφαρμογή μηχανισμών για τη διαχείριση αιτημάτων πρόσβασης υποκειμένων δεδομένων (DSAR), που επιτρέπουν στα άτομα να έχουν πρόσβαση στα προσωπικά τους δεδομένα.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Active Directory για να διαχειριστείτε αιτήματα πρόσβασης.
    - Βιβλιογραφικές αναφορές:
        - Azure Active Directory
- **Διόρθωση, διαγραφή και περιορισμός** : Παροχή διαδικασιών για τα υποκείμενα των δεδομένων για διόρθωση, διαγραφή ή περιορισμό της επεξεργασίας των προσωπικών τους δεδομένων.
    - **Azure Integration** : Χρησιμοποιήστε το Azure Data Factory για να αυτοματοποιήσετε τις διαδικασίες διαχείρισης δεδομένων.
    - Βιβλιογραφικές αναφορές:
        - Azure Data Factory

2. Διαχείριση συναίνεσης

- **Λήψη συγκατάθεσης** : Διασφάλιση ότι η συγκατάθεση λαμβάνεται από τα υποκείμενα των δεδομένων με σαφή και διαφανή τρόπο, με δυνατότητα εύκολης ανάκλησης της συγκατάθεσης.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε την Πολιτική Azure για να επιβάλετε τη συμμόρφωση με τη διαχείριση συναίνεσης.
    - Βιβλιογραφικές αναφορές:
        - Πολιτική Azure
- **Σημειώσεις απορρήτου** : Παροχή σαφών και προσβάσιμων ειδοποιήσεων απορρήτου που ενημερώνουν τα υποκείμενα των δεδομένων σχετικά με την επεξεργασία των προσωπικών τους δεδομένων.
- **Ενσωμάτωση Azure** : Χρησιμοποιήστε την Προστασία πληροφοριών Azure για την επισήμανση και την προστασία των εγγράφων.

Commented [FS13]: τα αιτήματα πρόσβασης δεν αφορούν το έργο ως μια ενδιάμεση πλατφόρμα καθαρισμού/εμπλουτισμού αλλά τις πηγές μας και τους προορισμούς μας

Commented [KA14R13]: Συμφωνώ με το σχόλιο. Στο αρχείο "Master_data _cleaning" αναφέρεται ότι τα αιτήματα πρόσβασης αφορούν τις πηγές και τους προορισμούς και όχι την ενδιάμεση πλατφόρμα.

Commented [FS15]: Πρέπει να παρέχουμε δυνατότητα λήθης (διαγραφή κλπ) στα ευαίσθητα δεδομένα που έχουν περάσει στο σύστημα του έργου
Αυτό μπορεί να γίνει με procedures που θα μεταβάλουν όλα τα ενδιάμεσα layers

Commented [KA16R15]: Συμφωνώ με το σχόλιο. Στο αρχείο "HEDNO Data Cleansing Technical Proposal_For Submission_01042024_FINAL" αναφέρεται η ανάγκη για δυνατότητα λήθης μέσω διαδικασιών που θα επηρεάζουν όλα τα ενδιάμεσα επίπεδα.

Commented [FS17]: Δεν αφορά το έργο αλλα τον οργανισμό

Commented [KA18R17]: Συμφωνώ με το σχόλιο. Στο αρχείο "Matching process" αναφέρεται ότι αυτό είναι ζήτημα του οργανισμού και όχι του έργου.

- Βιβλιογραφικές αναφορές:
    - Προστασία πληροφοριών Azure

3. Ειδοποίηση παραβίασης δεδομένων

- **Ανίχνευση και αναφορά** : Εφαρμογή διαδικασιών για τον έγκαιρο εντοπισμό, αναφορά και διερεύνηση παραβιάσεων δεδομένων.
    - **Azure Integration** : Χρησιμοποιήστε το Azure Security Center για ανίχνευση απειλών σε πραγματικό χρόνο.
    - Βιβλιογραφικές αναφορές:
        - Κέντρο Ασφαλείας Azure
- **Απαιτήσεις ειδοποίησης** : Διασφάλιση ότι οι παραβιάσεις δεδομένων αναφέρονται στις αρμόδιες αρχές και τα επηρεαζόμενα άτομα εντός 72 ωρών.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε τις εφαρμογές Azure Logic για να αυτοματοποιήσετε τις ροές εργασίας ειδοποιήσεων παραβίασης.
    - Βιβλιογραφικές αναφορές:
        - Εφαρμογές Azure Logic

4. Συμφωνίες Επεξεργασίας Δεδομένων

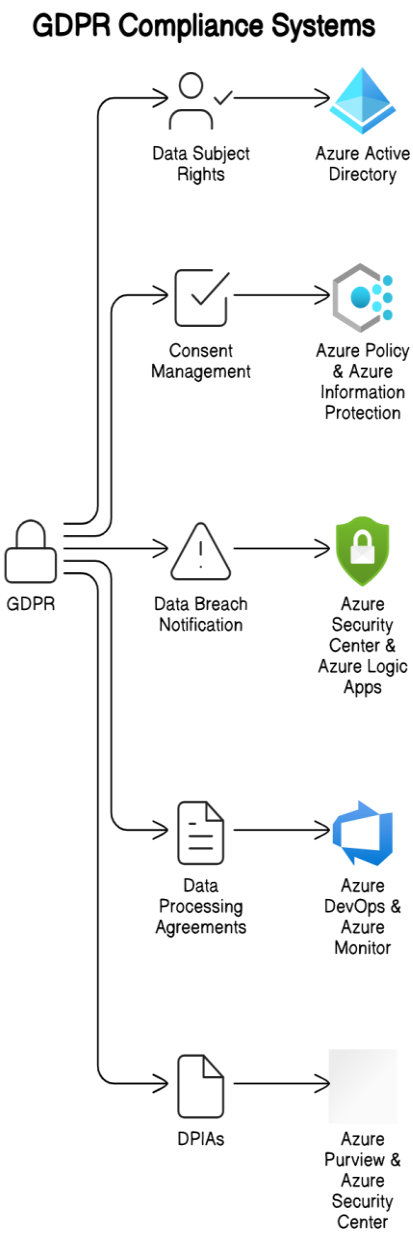
- **Συμμόρφωση τρίτων μερών** : Σύναψη συμφωνιών επεξεργασίας δεδομένων με όλους τους τρίτους φορείς επεξεργασίας για τη διασφάλιση της συμμόρφωσης με τον GDPR.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure DevOps για να διαχειριστείτε τις συμβάσεις και την τεκμηρίωση συμμόρφωσης.
    - Βιβλιογραφικές αναφορές:
        - Azure DevOps
- **Τακτικές αναθεωρήσεις** : Διενέργεια τακτικών επιθεωρήσεων και ελέγχων τρίτων επεξεργαστών για τη διασφάλιση της συνεχούς συμμόρφωσης.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Monitor για να παρακολουθείτε μετρήσεις συμμόρφωσης.
    - Βιβλιογραφικές αναφορές:
        - Azure Monitor

Commented [FS19]: Νομίζω είναι out of scope για το έργο

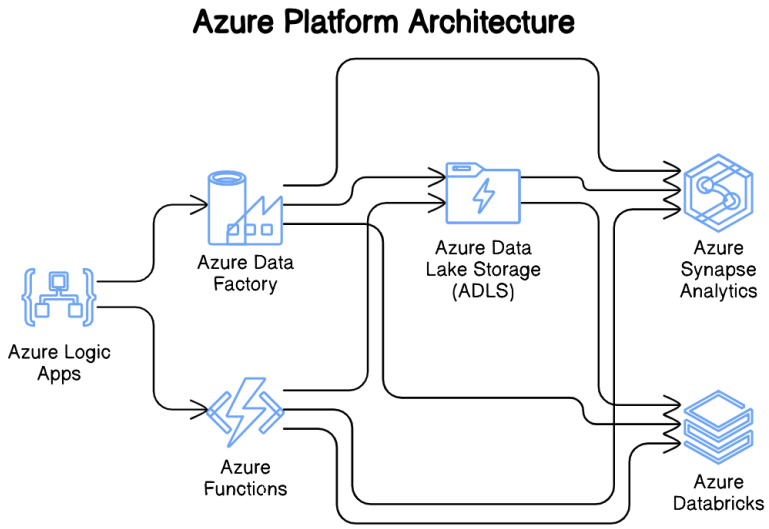
Commented [KA20R19]: Συμφωνώ με το σχόλιο. Στο αρχείο "WEMETRIX_deh_DATA_CLEANSING_PROPOSAL_04052023_V2" αναφέρεται ότι ορισμένα ζητήματα είναι εκτός πεδίου εφαρμογής του έργου.

5. Εκτιμήσεις Επιπτώσεων Προστασίας Δεδομένων (ΕΑΠΔ)

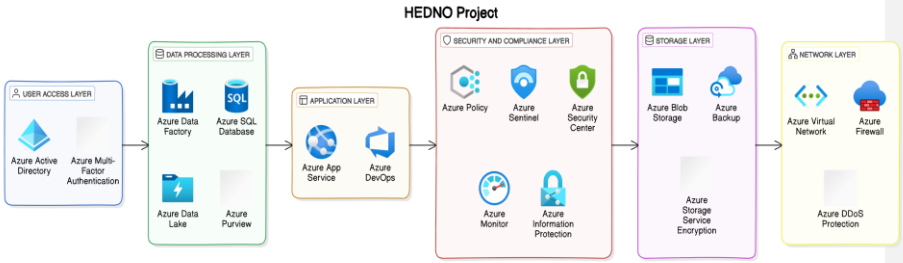
- **Διενέργεια ΕΑΠΔ** : Διεξαγωγή ΕΑΠ για δραστηριότητες επεξεργασίας που ενέχουν υψηλούς κινδύνους για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Purview για διαχείριση και αξιολόγηση δεδομένων.
    - Βιβλιογραφικές αναφορές:
        - Azure Purview
- **Μετριασμός κινδύνου** : Εντοπισμός και μετριασμός κινδύνων που σχετίζονται με δραστηριότητες επεξεργασίας δεδομένων για τη διασφάλιση της συμμόρφωσης με τον GDPR.
    - **Ενσωμάτωση Azure** : Χρησιμοποιήστε το Azure Security Center για να εντοπίσετε και να μειώσετε τους κινδύνους.
    - Βιβλιογραφικές αναφορές:
        - Κέντρο Ασφαλείας Azure
    - **Azure GDPR**


GDPR Compliance Systems
GDPR
Data Subject Rights
Azure Active Directory
Consent Management
Azure Policy & Azure Information Protection
Data Breach Notification
Azure Security Center & Azure Logic Apps
Data Processing Agreements
Azure DevOps & Azure Monitor
DPIAs
Azure Purview & Azure Security Center

- **Γενική Αρχιτεκτονική Επισκόπηση**



- **Ειδική Επισκόπηση έργου**



συμπέρασμα

Αυτή η έκθεση περιγράφει τις βασικές απαιτήσεις Ασφάλειας Δεδομένων, Ασφάλειας Συστήματος και GDPR που σχετίζονται με το έργο του ΔΕΔΔΗΕ. Η ενσωμάτωση με τις τεχνολογίες Azure παρέχει ισχυρές λύσεις για την κάλυψη αυτών των απαιτήσεων, διασφαλίζοντας ότι το έργο διατηρεί τα υψηλότερα πρότυπα ασφάλειας και συμμόρφωσης.

Η ομάδα Incelligent θα πρέπει να επανεξετάσει και να διασφαλίσει ότι όλα τα καθορισμένα μέτρα εφαρμόζονται και διατηρούνται καθ' όλη τη διάρκεια του κύκλου ζωής του έργου για την τήρηση των υψηλότερων προτύπων ασφάλειας και συμμόρφωσης. Εάν χρειάζονται

Commented [FS21]: τα διαγράμματα αυτα δεν χρειάζονται εδώ

Commented [KA22R21]: Συμφωνώ με το σχόλιο. Στο αρχείο "AnyConv.com__Suggested_Architecture_12062023_v03" αναφέρεται ότι τα συγκεκριμένα διαγράμματα δεν είναι απαραίτητα.

περαιτέρω λεπτομέρειες ή διευκρινίσεις, ανατρέξτε στα σχετικά αρχεία ή επικοινωνήστε με τους σχετικούς ενδιαφερόμενους φορείς.

Σχετικά Αρχεία κατά Απαίτηση

File	Data Security	System Security	GDPR
Data_Cleansing_PartI_byPredicta - Brief_Description_vGeneric.pdf	X		
IBM DATASTAGE - 3 MATCHING PROCESS.pdf	X		
Matching process.docx	X		
Blocking and Matching criteria.docx	X		
IBM DATASTAGE - 4 GOLDEN RECORD.pdf	X		
HEDNO_MASTER_DATA_MATRIX.xlsx	X		X
ExportedEstimateDEDDHE_staging3.xlsx	X		X
Σεμινάρια - Incelligent.xlsx	X		X
PPC Mnemosyne Web Service for Deltas.pdf	X		
Αρχιτεκτονική.docx		X	
Suggested_Architecture_12062023_v03.pdf		X	
HEDNO Deliverable 1_assignments.pdf		X	
EAPD_CNIL_gr.docx			X
Τεχνικές Προδιαγραφές Παραδοτέων.docx			X
Π1-Αναλυτική Μελέτη Μεθοδολογικής Προσέγγισης-Draft20240605.docx			X
ΠΕΡΙΓΡΑΦΗ ΥΠΗΡΕΣΙΑΣ_18042023_v08.docx			X
HEDNO Data Cleansing Tecnical Proposal_For Submission_01042024_FINAL.docx			X
Wemetrix_PPC data Clensing_Documentation_20231124.pdf			X
WEMETRIX*ΔΕΗ*DATA_CLEANSING_PROPOSAL_04052023_V2.docx			X
512436-dplps-master-data-cleansing-project-diakhryksh-20240301.signed-ef-1.pdf			X
WPs_timeline.png			X

Commented [FS23]: τι ειναι αυτά? τα deliverables αρχεία θα δωθούν στο τέλος του έργου

Commented [KA24R23]: Συμφωνώ με το σχόλιο. Στο αρχείο "AnyConv.com__HEDNO Deliverable 1_assignments" αναφέρεται ότι τα παραδοτέα θα δοθούν στο τέλος του έργου.
Αυτός είναι ένας πίνακας μήτρας των σχετικών αρχείων που αφορούν την Ασφάλεια Δεδομένων, την Ασφάλεια Συστήματος και το GDPR για την ενημέρωσή σας.